Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Currently amended) A method for detecting unauthorized intrusion in a network system, comprising the steps of:

receiving packet level activity information from the network;

collecting sequential samples of sorted ~~sorting~~ port specific activity information from the received packet level activity information ~~by~~ for each IP/user;

converting packet level ~~the sorted IP/user port specific~~ activity ~~information to~~ into human ~~behavioral measures of intent;~~ behaviors and activities for each IP/user;

converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user;

monitoring sequential determinations of the ~~monitoring the~~ converted human intent behavioral measures, for the duration that each IP/user is in the network, wherein the monitoring step includes determining new and previously undetected misuse behaviors as indicated by increased intent levels of expertise and deception; and

executing at least one of a network connection blocking action or ~~a tracking action based upon the monitored human behavioral measures~~ passive gathering of tracked intent information for any given IP/user if monitored expertise and deception measures exceed intent thresholds underlying non-misuse network activity.

2.   (Original) The method according to claim 1, wherein the step of monitoring includes:

identifying presence of at least one activity from the port specific activity information;

assigning a binary representation (1 = present, 0=absent) to the at least one identified

activity; and

generating an assessment based upon the binary rating.

3.   (Original) The method according to claim 2, wherein the step of generating an

assessment includes associating the binary rating with an assessment based upon predetermined

behavioral criteria.

4.   (Original) The method according to claim 3, wherein the step of generating an

assessment includes mapping the assessment on at least one two-dimensional grid.

5.   (Original) The method according to claim 4, wherein the step of mapping occurs

dynamically and in real-time.

6.   (Currently Amended) The method according to claim 2, wherein the step of generating

an assessment includes generating a profile of the IP/user based upon the monitored behavioral

measures.

7.   (Original) The method according to claim 2, wherein the step of generating an

assessment is carried out utilizing a back propagation network.

8. (Original) The method according to claim 7 wherein the back propagation network includes psychological assessment information.

9. (Original) The method according to claim 2, wherein the assessment is one of high deception/high expertise, high deception/low expertise, low deception/high expertise and low deception/low expertise.

10. (Original) The method according to claim 1, wherein the blocking action includes sending a blocking command to a firewall for blocking further network access.

11. (Original) The method according to claim 1, wherein the tracking action includes storing activity information in a tracking module.

12. (Currently Amended) A system for preventing unauthorized intrusion in a network system, comprising:

a traffic sorter that receives a copy of the network activity and <u>sorts all activities by IP/User for the purpose collecting sequential samples of each IP/user's activities/behaviors:</u>

an activity monitor operatively coupled to the traffic sorter for <u>sequentially</u> monitoring converted human <u>intent</u> behavior <u>behaviors and activities</u> measures by IP/users[;]<u>:</u>

an inter-port fusion module operatively coupled to the activity monitor that fuses

assessments from one or more assessment engines that monitor behavior measures by IP/User[;]:

and

an outcome director operatively coupled to the inter-port fusion monitor that determines

whether to block or track IP/users on a specific IP/User basis based upon assessed behavioral

measures of intent.

13. (Currently Amended) The system according to claim 12, wherein the activity monitor

includes at least one dedicated behavior monitor.

14. (Currently Amended) The system according to claim 13, wherein, the at least one

dedicated behavior monitor includes an activity /behavior analysis module, an activity translator

module and an assessment module.

15. (Currently Amended) The system according to claim 14, wherein the assessment module

includes a trained back propagation network.

16. (Original) The system according to claim 15, wherein the back propagation network

includes psychological assessment information.

17.   (Currently Amended) The system according to claim 14, wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network into IP/Users.

18.   (Currently Amended) The system according to claim 14, wherein the activity monitor monitors the port and across-portspecific activity information.

19.   (Currently Amended) The system according to claim 14, wherein the activity translator module assigns a binary rating based upon presence (1) or absence (0) of at least one activity/behavior detected by the packet level analysis module.

20.   (Currently Amended) The system according to claim 19, wherein the assessment module generates an assessment of levels of expertise and deception present in any sample of an IP/User's overall activities/behaviors for a collection interval.

21.   (Currently Amended) The system according to claim 19, wherein the assessment module maps the assessment result utilizing at least one of a two dimensional grid or X dimensional grid for optional real-time viewing of a user's intent for each sequential collection interval.

22.   (Original) The system according to claim 20, wherein an outcome director initiates at least one of a blocking command or a tracking command based upon the assessment result.

23.   (Original) The system according to claim 22, wherein the blocking command is directed to a system firewall.

24.   (Currently Amended) The system according to claim 23 in which a blocking command results in the loss of the connection between an IP/User and the network and the storage storage of all relevant session data up to the point of forced loss of the IP/User's connection to the network.

25.   (Original) The system according to claim 22, wherein the tracking command is directed to a tracking module.

26.   (Original) The system according to claim 24, wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's harmful intent activities and at least one intent assessment during a session.

27.   (Original) The system according to claim 26, wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked or blocked.

28.   (Original) The system according to claim 27, wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion.

29.   (Original) The system according to claim 28, wherein at least one of a blocking or

tracking action is executed based upon an output from the comparison module.

30.   (Currently Amended) A system for detecting unauthorized intrusion in a network system,

comprising:

sorting means for sorting <u>sequential samples of</u> IP/User specific activities/behaviors by

and across ports ;

conversion means for converting the IP/User specific activities/behaviors to behavioral

measures of <u>expertise and deception as measures of underlying</u> intent <u>for each IP/user</u>;

monitoring means operatively coupled to the sorting means for monitoring <u>sequential</u>

<u>determinations of</u> the <u>converted</u> behavioral measures <u>for the duration that each IP/user is in the</u>

<u>network and for determining new and previously undected misuse behaviors as indicated by</u>

<u>increased intent levels of expertise and deception;</u> and

assessing means operatively coupled to the monitoring means for generating separate and

independent IP/user assessments based upon the behavior measures.

31.   (Currently Amended) A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for

preventing unauthorized intrusion into a computer network, the computer program product

comprising:

computer readable program code configured to cause the computer to process a

copy of network activity in real-time to collect sequential samples of sorted ~~sort~~ port specific and

non-port specific activity information for each IP/user from packet level activity information

received by the computer network; .

computer readable program code configured to cause the computer to covert the

~~port and non-port specific~~ packet level activity ~~information~~ into human behaviors and activities

for each IP/user and convert the sorted IP/user behavioral activities into behavioral measures of

expertise and deception as measures of underlying intent for each IP/user ~~behavioral measures of~~

~~intent separately and independently for each IP/user~~;

computer readable program code configured to cause the computer to monitor ~~the~~

~~behavior measures by IP/user~~ sequential determinations of the converted human intent

behavioral measures, for the duration that each IP/user is in the network, wherein the montoring

step includes determining new and previously undetected misuse behaviors as indicated by

increased intent levels of expertise and deception; and

computer readable program code configured to cause the computer to execute at

least one of a network connection blocking action or ~~a tracking action for the IP/user if assessed~~

~~behavioral measures indicate a threat intent~~ passive gathering of tracked intent information for

any given IP/user if monitored expertise and deception measures exceed intent thresholds

underlying non-misuse network activity.

32.   (Currently Amended) The method according to claim 1, wherein the step of receiving the port and non-port specific specific activity/behavior information includes creating a copy of the network activity sorted by users.

33.   (Previously Added) The method according to claim 1, further including the step of sorting non-port specific activity information from the received packet level activity information by IP/user; and converting the non-port specific activity information to human behavioral measures of intent.